IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Number:	10/679,654
Filing Date:	10/6/2003
Applicant(s):	Keith Bryan Knight
Entitled:	TUNELLING NON-HTTP STREAMS
	THROUGH A REVERSE PROXY
Examiner:	John B. Walsh
Group Art Unit:	2151
Attorney Docket No.:	LOT9-2003-0023 (7321-9U)

Mail Stop AF
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Sir:

Appellants request that a Panel Review of the final rejection be performed in the above identified application.

REMARKS

I. Prosecution History

Presently, claims 1 through 13 are pending in the Patent Application. Claims 1, 6, and 9 are independent claims. In a first non-final office action dated June 29, 2005, the Examiner rejected each of claims 1 through 13 under 35 U.S.C. § 102(b) as being anticipated by U.S.

Patent No. 6,081,900 to Subramaniam et al. (Subramaniam). The Applicants traversed the

Examiner's rejections noting that Subramaniam teaches tunneling non-hypertext transfer protocol

(HTTP) data through a reverse proxy within HTTP messages while the claims of the Patent

Application explicitly required that non-HTTP data is passed through the reverse proxy without

encapsulating the non-HTTP data within HTTP messages.

In a second non-final office action issued on July 17, 2006, claims 1 through 13 were

newly rejected under 35 U.S.C. § 103(a) as being a mere obvious variation of Subramaniam.

Again, the Applicants traversed the Examiners noting that Subramaniam teaches tunneling non-

hypertext transfer protocol (HTTP) data through a reverse proxy within HTTP messages while

the claims of the Patent Application explicitly required that non-HTTP data is passed through the

reverse proxy without encapsulating the non-HTTP data within HTTP messages. In response, in

a Final Office Action dated December 21, 2006, the Examiner again rejected claims 1 through 13

under 35 U.S.C. § 103(a) as being anticipated by Subramaniam.

II.   Invention Summary

The Applicant has invented is a method, system and apparatus for tunneling non-HTTP

streams through a reverse proxy. In the Applicants' invention, a socket connection can be

established with a reverse proxy. Based upon the establishment of the socket connection, the

socket can be passed to a non-HTTP data stream handler. The non-HTTP data stream handler

can maintain the open socket connection and can write non-HTTP data streams over the socket

without encapsulating the non-HTTP data within an HTTP message. The non-HTTP data stream

handler can continue to exchange the non-HTTP data over the open socket until finished.

Subsequently, the non-HTTP data stream handler can close the socket. Significantly, and unlike

prior art HTTP tunneling implementations, in the Applicants' invention, the non-HTTP data can

be exchanged over the secured connection without encapsulating the non-HTTP data within

HTTP messages.

III.   Cited Art - Subramaniam

Subramaniam relates to securely accessing a network from an external client. Requests

for access to confidential data are redirected from a target server to a border server, after which a

secure sockets layer (SSL) connection between the border server and the external client carries

user authentication information. After the user is authenticated to the network, requests may be

redirected back to the original target server. Web pages sent from the target server to the

external client are scanned for non-secure uniform resource locators (URLs) such as those

containing the prefix "http://" and those URLs are modified to make them secure. In one

embodiment taught within Subramaniam, tunneling is used for the redirection.

Figure 1 of Subramaniam is representative of the Subramaniam system. As shown in

Figure 1, secure data (shown as elements 134 and 138) is passed to a target server (shown as

element 104) through a border server (shown as element 106). The exchange of the secure data

from the border server to the target server is performed by using tunneling and is shown as

"Secure Data in Tunnel 138" within Figure 1. Figure 2 of Subramaniam clarifies the operation

of the system of Figure 1 by stating "transmit secure data from target server through border

server tunnel to user/client" in the method step labeled step 136 in Figure 2.

Importantly, as discussed in column 3, lines 40 through 50 of Subramaniam, column 3

line 66 through column 4, line 19 of Subramaniam, column 7, lines 1 through 35 of

Subramaniam, and column 8 lines 13 through 23 of Subramaniam, the border manager of the

Subramaniam system can re-write the URL of an incoming request associated with secure data from an "http" header to a "https" header in order to invoke "HTTPS" treatment. As it is understood in the art, HTTPS is HTTP over an SSL connection. The messages exchanged in HTTPS are HTTP messages. The HTTP messages, however, are exchanged using SSL connectivity.

IV.   Argument

Subramaniam teaches tunneling non-hypertext transfer protocol (HTTP) data through a reverse proxy <u>within HTTP messages</u> while the claims of the Patent Application explicitly require that non-HTTP data is passed through the reverse proxy <u>without encapsulating the non-HTTP data within HTTP messages</u>. Clearly, the "without encapsulating said non-HTTP data within HTTP messages" is not shown by Subramaniam because Subramaniam requires the use of HTTP messages inherent to HTTP. Thus, the Applicants respectfully believe that Subramaniam cannot be held to teach each and every recited limitation of the claims of the Applicants' Patent Application.

As noted in the Applicants' response to the non-final office action dated July 17, 2006, the Applicants do not agree that the cited portion of Subramaniam--namely column 7, lines 65-67-- stands for the proposition that "non-HTTP data" is exchanged over the secure connection without encapsulating the non-HTTP data in an HTTP message. Rather, Subramaniam quite clearly contemplates that non-HTTP data is encapsulated within secure HTTP messages as stated in column 7, line 25. This stands in direct contradiction to the Applicants' claim language.

In the Final Office Action, the Examiner stated

The examiner disagrees since column 7, line 25 of Subramaniam does not disclose encapsulating non-HTTP data, but discloses changing the protocol from

HTTP to HTTPS. Subramaniam et al. discloses one of ordinary skill in the art
could use other protocols as FTP, for exchanging data (column 7, lines 65-67).
Subramaniam does not disclose that the FTP is encapsulated within HTTP data,
thus Subramaniam discloses the applicant's claimed limitation of "responsive to
establishing said connection ,maintaining said connection exchanging no-HTTP
data over said secured connection without encapsulating said non-HTTP data
within HTTP messages," since the use of FTP data is non-HTTP data.

This response is nonsensical as the Examiner essentially does not rely upon a teaching of

Subramaniam, but the Examiner relies upon what is NOT taught by Subramaniam in direct

contravention of the most basic requirements of establishing a prima facie case of obviousness

set forth in M.P.E.P. § 2142 in which it is stated, ."[T]he prior art reference (or references when

combined) must teach or suggest all the claim limitations". In any case, the Examiner has failed

to refer to a teaching in Subramaniam for all of the claim limitations of the Applicants' claims

nor has the Examiner provided a legitimate motivation to combine sufficient to satisfy the legal

standard of obviousness set forth in M.P.E.P. § 2142.

Respectfully submitted,

Date: October 17, 2006
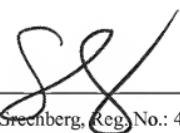
Steven M. Greenberg, Reg. No.: 44,725
Attorney for Applicant(s)
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, Florida 33487
Customer No. 46321
Tel: (561) 922-3845
Fax: (561) 244-1062